
MODULE 1: DATA FOUNDATIONS

CT ACADEMY | DATA ACTION LAB

2. DATA ETHICS

DATA FOUNDATIONS

MOTIVATION AND POLICY DRIVERS

Unethical and irresponsible handling of data assets and A.I. can have a broad range of consequences:

- Decision-making and policies resulting in harms (e.g., stigma, financial loss, etc.) to individuals and communities
- Violations of personal privacy
- A.I. models that are difficult to understand and can behave in unintended manners
- Loss of public trust, hindering the ability to meaningfully engage with Canadians

Policy drivers for ethical handling of data

- Federal Data Strategy Roadmap / 2023–2026 Data Strategy for the Federal Public Service
- Departmental Data Strategy – Ethical use of data as an asset
- Canada’s Digital Ambition 2022

Policy drivers for ethical handling of Indigenous data

- UNDRIP / UNDA / UNDA Action Plan
- Departmental Reconciliation Strategy
- 2023–2026 Data Strategy for the Federal Public Service

Policy drivers for responsible use of A.I.

- Federal Responsible A.I. Guiding Principles
- TBS Directive on Automated Decision-Making
- Government of Canada Digital Standards: Playbook

COMMONLY USED TERMS

- Data ethics
- Governance
- Consent
- Bias and discrimination
- Inclusiveness
- Fairness
- Accountability

WHAT ARE ETHICS?

Broadly speaking, ethics refers to the study and definition of right and wrong conducts.

We all have a personal ethical system, don't we?

- be honest
- be fair
- be objective
- be responsible
- be compassionate
- etc.



WHAT ARE DATA ETHICS?

Data ethics is a branch of ethics that evaluates data practices, including the **collection, generation, analysis, and dissemination** of data, that have the potential to adversely impact people and society.

Mission 3 (Enabling Data-Driven Services) of the 2023-26 data strategy refresh from TBS, states that GoC entities will ensure...

“... the responsible, ethical and transparent sharing and use of data are key to enabling the delivery of better services to people in Canada.”

THE NEED FOR ETHICS

When large scale data collection first became possible, there was to some extent a “**Wild West**” mentality to data collection and use. Whatever wasn’t proscribed from a technological perspective was allowed (if not mandatory).

Now, however, professional codes of conduct are being devised, for example, for data scientists, which outline responsible ways to practice data science – i.e., ways that are **legitimate** rather than fraudulent, as well as **ethical**, rather than unethical.

THE NEED FOR ETHICS

Although this puts some **extra** responsibility onto data scientists, it also provides them with protection from people who hire them to carry out data science in questionable ways – **they can refuse on the grounds that it is against their professional code of conduct.**

Does your organization have a code of ethics for its data scientists or other data professionals? For its employees?

BEST PRACTICES

“Do No Harm”: data collected from an individual **should not be used to harm** the individual. This may be difficult to apply in practice.

Informed Consent: covers a wide variety of ethical questions, but mainly:

- individuals must **agree to the collection and use** of their data
- individuals must have a **real understanding of what they are consenting to**, and of **possible consequences** for them and others.

BEST PRACTICES

Respect “Privacy”: dearly-held principle. Excessively hard to maintain in the age of constant trawling of the Internet for personal data.

Keep Data Public: another aspect of data privacy – some (all? most? any?) data should be kept **public**.

Opt-In/Opt-Out: informed consent requires the ability to **not consent** (to opt out).

- tacit vs. stated consent

BEST PRACTICES

Anonymize Data: removal of identifying fields from the dataset prior to analysis.

“Let the Data Speak”:

- no cherry picking
- importance of validation
- correlation and causation
- repeatability

EXERCISES

In groups, discuss how data ethics best practices are applied in your organizations.

“And yes, **transparency is also the trick to protecting privacy**, if we empower citizens to notice when neighbors infringe upon it. Isn’t that how you enforce your own privacy in restaurants, where people leave each other alone, because those who stare or listen risk getting caught?”

David Brin, *The Transparent Society*

BIAS

A **cognitive bias** is a systematic error in thinking that occurs when people get information in the world around them, and their processing and interpreting of this information affects the decisions and judgments that they make.

The human brain is powerful but subject to imperfections. Cognitive biases are often a result of the brain's attempt to **simplify information processing**. They often work as rules of thumb that help us make sense of the world and reach decisions with relative speed.

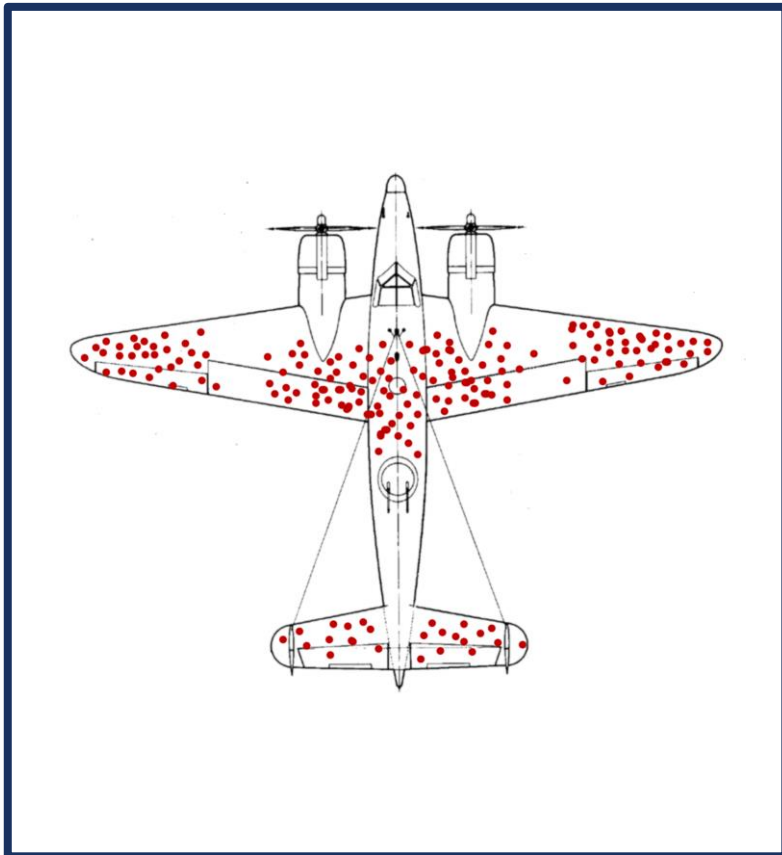


During WWII, mathematician **A. Wald** undertook a study to help protect Allied bombers flying over enemy territory.

Data included: the **number** and **location** of **bullet holes** on returning aircraft, and the goal was to use this information to determine where to add armor to best protect the plane's structure.

A chart was created to show where the maximum number of bullet holes were located on **returning aircraft**. This chart showed greatest damage on the **aircraft extremities**, not on the main wing and tail spars, engines, and core fuselage areas.

BIAS



As such, the Air Ministry wanted to add armor to the **extremities**. Wald suggested they were **dead wrong**.

To avoid “**survivorship bias**”, armor should be added to the areas with the **fewest holes**: if no returning planes had holes in their wing spars and engines, then even a few holes in those locations were **deadly**.

Take-Away: the data that is missing may be as important to story than the data that is there. Storytelling is not always an obvious endeavour.

1. Anchoring bias.

People are **over-reliant** on the first piece of information they hear. In a salary negotiation, whoever makes the first offer establishes a range of reasonable possibilities in each person's mind.



2. Availability heuristic.

People **overestimate the importance** of information that is available to them. A person might argue that smoking is not unhealthy because they know someone who lived to 100 and smoked three packs a day.



3. Bandwagon effect.

The probability of one person adopting a belief increases based on the number of people who hold that belief. This is a powerful form of **groupthink** and is reason why meetings are often unproductive.



4. Blind-spot bias.

Failing to recognize your own cognitive biases is a bias in itself. People notice cognitive and motivational biases much more in others than in themselves.



5. Choice-supportive bias.

When you choose something, you tend to feel positive about it, even if that **choice has flaws**. Like how you think your dog is awesome – even if it bites people every once in a while.



6. Clustering illusion.

This is the tendency to **see patterns in random events**. It is key to various gambling fallacies, like the idea that red is more or less likely to turn up on a roulette table after a string of reds.



7. Confirmation bias.

We tend to listen only to information that confirms our **preconceptions** – one of the many reasons it's so hard to have an intelligent conversation about climate change.



8. Conservatism bias.

Where people favor prior evidence over new evidence or information that has emerged. People were **slow to accept** that the Earth was round because they maintained their earlier understanding that the planet was flat.



9. Information bias.

The tendency to **seek information when it does not affect action**. More information is not always better. With less information, people can often make more accurate predictions.



10. Ostrich effect.

The decision to **ignore dangerous or negative information** by “burying” one's head in the sand, like an ostrich. Research suggests that investors check the value of their holdings significantly less often during bad markets.



11. Outcome bias.

Judging a decision based on the **outcome** – rather than how exactly the decision was made in the moment. Just because you won a lot in Vegas doesn't mean gambling your money was a smart decision.



12. Overconfidence.

Some of us are **too confident about our abilities**, and this causes us to take greater risks in our daily lives. Experts are more prone to this bias than laypeople, since they are more convinced that they are right.



13. Placebo effect.

When **simply believing** that something will have a certain effect on you causes it to have that effect. In medicine, people given fake pills often experience the same physiological effects as people given the real thing.



14. Pro-innovation bias.

When a proponent of an innovation tends to **overvalue its usefulness** and undervalue its limitations. Sound familiar, Silicon Valley?



15. Recency.

The tendency to weigh the **latest information** more heavily than older data. Investors often think the market will always look the way it looks today and make unwise decisions.



16. Salience.

Our tendency to focus on the **most easily recognizable features** of a person or concept. When you think about dying, you might worry about being mauled by a lion, as opposed to what is statistically more likely, like dying in a car accident.



17. Selective perception.

Allowing our expectations to **influence how we perceive** the world. An experiment involving a football game between students from two universities showed that one team saw the opposing team commit more infractions.



18. Stereotyping.

Expecting a group or person to have certain qualities without having real information about the person. It allows us to quickly identify strangers as friends or enemies, but people tend to **overuse and abuse** it.



19. Survivorship bias.

An error that comes from focusing only on surviving examples, causing us to **misjudge a situation**. For instance, we might think that being an entrepreneur is easy because we haven't heard of all those who failed.



20. Zero-risk bias.

Sociologists have found that **we love certainty** – even if it's counterproductive. Eliminating risk entirely means there is no chance of harm being caused.



EXERCISE

Translate the cognitive biases to analytical contexts.

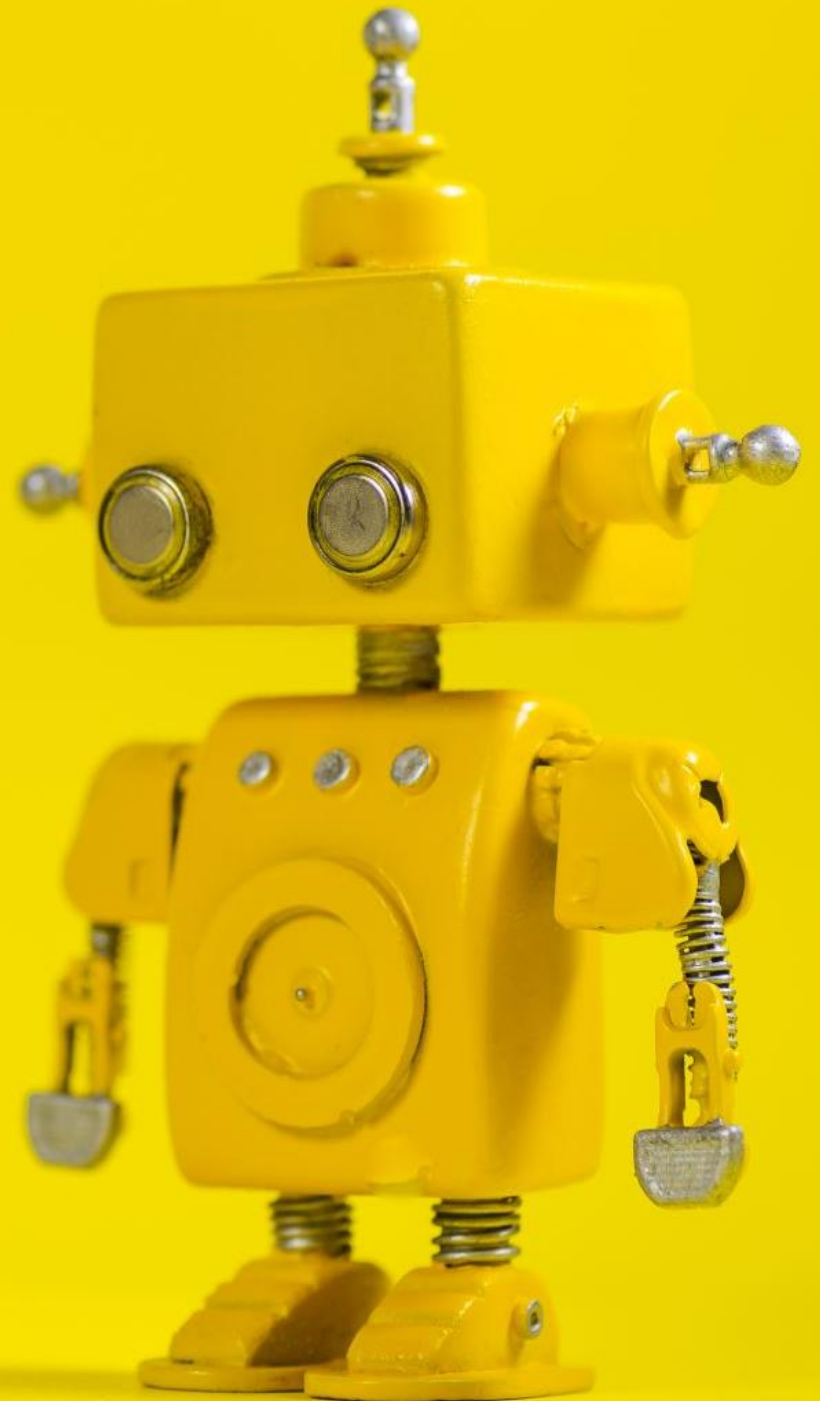
What cognitive biases are you, your team, and your organization most susceptible to?

Least?

ETHICS IN A.I.

The explosion in the use of “**Artificial Intelligence**” has required the creation of GoC guidance on the responsible use of A.I.

The GoC policy also includes the *Directive of Automated Decision-Making* and the *Guide on the use of generative A.I.*



CASE STUDY: AMAZON HIRING A.I.

Your company is always looking for the most talented people, especially for technical positions.

Corporate policy **supports** diversity and inclusion.

The hiring process is time-consuming, and you are concerned about **personal biases** of panel members influencing the decisions.

With the help of an outstanding A.I. team, you **automate** this process.

The A.I.-assisted processes finds talented people, who fit into the organizational culture, and who like their jobs (low turnover).

CASE STUDY: AMAZON HIRING A.I.

But... more likely to get hired if your name was **Jared** and you played **lacrosse**.

A.I. was behaving in a **biased manner**, not recommending women be hired.

Amazon was not confident they could **remove the bias** or identify biased behaviours in the future, so they project was **scrapped**.



A.I. ETHICS GUIDING PRINCIPLES

Uses:

- privacy and security
- transparency
- accountability
- methodology and data quality
- model fairness
- model explainability
- indigenous data sovereignty



DATA ETHICS

Data ethics questions:

- Who, if anyone, owns data?
- Are there limits to how data can be used?
- Are there value-biases built into certain analytics?
- Are there categories that should not be used in analyzing personal data?
- Should some data be publicly available to all researchers?

Are there lessons to be learned from the First Nations Principles of OCAP[®]? (**ownership, control, access, possession**)



FIRST NATIONS DATA

First Nations Principles of **OCAP**[®]:

- **Ownership:** cultural knowledge, data, and information is owned by First Nations communities
- **Control:** First Nations communities have the right to control all aspects of research and information management that impact them
- **Access:** First Nations communities must have access to information and data about themselves no matter where it is held
- **Possession:** First Nations communities must have physical control of relevant data

DATA ETHICS

Some examples of data science ethics questions (University of Virginia's *Centre Data Ethics and Justice*):

- **who**, if anyone, owns data?
- are there **limits** to how data can be used?
- are there **value-biases** built into certain analytics?
- are there categories that should **never** be used in analyzing personal data?
- should some data be **publicly available** to **all** researchers?

EXERCISE

Answer the *Centre for Data Ethics and Justice* questions, as they apply to data used by your organization.

DATA ETHICS GUIDING PRINCIPLES

1. Public Benefit
2. Privacy and Security
3. Transparency
4. Accountability
5. Methodology and Data Quality
6. Indigenous Data Sovereignty

ETHICS AND THE DATA LIFECYCLE

Ethics must be considered at each stage of the **data lifecycle**.



Do we **acquire** data in an ethical and unbiased manner? It is **stored** safely? When we prepare it do we introduce biases? Is it **staged** safely and when we **present**, are we representing all the actors in a fair and ethical manner?

EXERCISE

In your own words, write out a list of guiding principles that could apply in the world of Government finance. Be specific and avoid generic words.

For example, “Cost center managers are accountable for providing an accurate representation of their finances at the end of each quarter”.

SUPPLEMENTAL MATERIAL

2. DATA ETHICS

PRINCIPLES AND STANDARDS

- Privacy Act
- Statistics Act
- Policy on Government Security
- Policy on Privacy Protection
- Privacy Impact Assessments
- Levels of Security
- Gender-Based Analysis+
- Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans
- Model Policy on Scientific Integrity
- Directive on Automated Decision-Making
- Disaggregated Data

WHAT ARE ETHICS?

Influential *Western* ethical theories:

- Kant's **golden rule** (do unto others as you would have them do unto you),
- **consequentialism** (the ends justify the means)
- **utilitarianism** (act in order to maximize positive effect)

Influential *Eastern* ethical theories:

- **Confucianism** (virtue from people and motives, not from outcomes)
- **Taoism** (case-by-case appropriateness of action determines morality)
- **Buddhism** (harmony and self-restraint to avoid causing harm)

WHAT ARE ETHICS?

Ubuntu ethical tradition:

- **tension** between individual and universal rights
- **global** context of life
- **solidarity**

Maori *tikanga*:

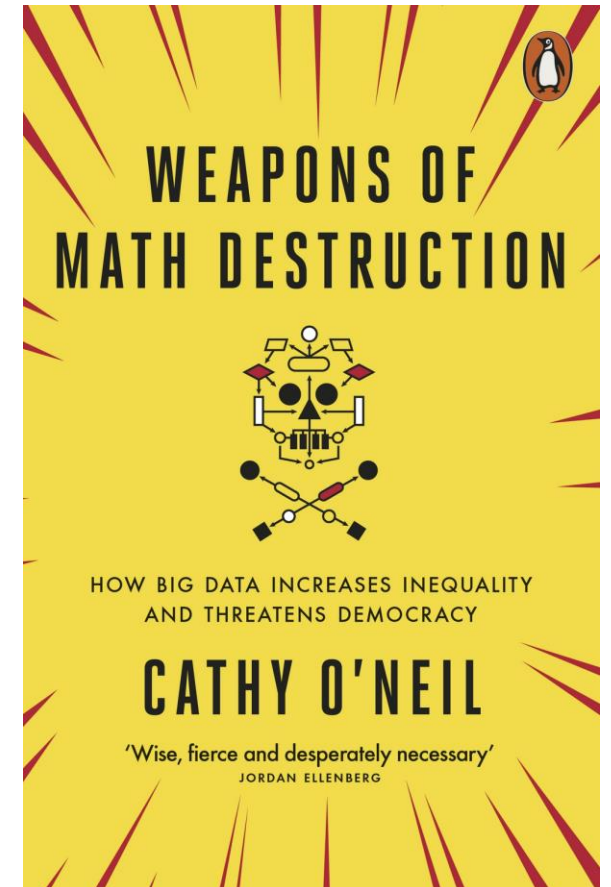
- connection with **spiritual** realm
- **respect** for all things
- **self-determination** and **reciprocity**

THE THREAT

In her book about data power, Dr. Cathy O’Neil presents several cautionary examples and tales.

“A computer program could speed through thousands of résumés [...] and sort them into neat lists [...]. This not only saved time but also was marketed as fair and objective. After all, it didn’t involve prejudiced humans digging through reams of paper, just machines processing cold numbers. [...]

The math-powered applications driving the data economy were based on choices made by fallible human beings. Some of these choices were no doubt made with the best intentions. Nevertheless, many of these models and algorithms encoded human prejudice, misunderstanding and bias into the software systems that increasingly managed our lives.”



LEGAL CONSIDERATIONS USING DATA

Profiling:

- are you using personal data to draw inferences that are unfair, unethical or discriminatory?

Surveillance:

- are people being placed in a perpetual line-up?

Liability:

- are you liable for what an A.I. does?

EMERGING LEGAL TRENDS

Canada

GoC: Algorithmic Impact Assessment prior to the production of any Automated Decision System

Privacy Commissioner (Personal Information Protection and Electronic Documents Act):

- Defines automated decision systems any tech that assists or replaces the judgment of humans.
- Need to give people an explanation of the prediction/recommendation, and how their personal info was used.

Europe

General Data Protection Regulation (GDPR)

Article 22: not subject to a decision based solely on automated processing (with exceptions)

Article 15: if subject to such a decision, have right to meaningful information about the logic involved.

CODES OF CONDUCT

A **code of conduct** is a set of rules outlining the norms, rules, and responsibilities or proper practices of an individual party or an organization (in medicine, we have the *Hippocratic Oath*).

Many professional organizations are starting to integrate data ethics into their **professional** designation's codes of conduct.

The Government of Canada has a general “[Values and Ethics Code for the Public Sector](#)” in which the use of data is **implied**.

The [2023-2026 Data Strategy](#) explicitly identifies ethical use of data as a guiding principle.

There are other subject-specific policies such as the [Tri-Council Policy on Ethical Conduct for Research Involving Humans](#), depending on areas of expertise.

PROTECTING AND SHARING CONFIDENTIAL DATA

Privacy is protected by laws and other measures including the [Statistics Act](#), the [Privacy Act](#), the [Directive on Security Management](#) and by [GoC Levels of Security](#).

In short, the data in documents/information with a higher classification rating than “unclassified” can **only be shared with personnel with the relevant level of screening** and on a “**need to know**” basis, with documents being held at a site with the appropriate organization screening.

Type	Information and assets	Organization screening	Personnel screening
Classified	Top Secret	Facility security clearance (Top Secret)	Top Secret
Classified	Secret	Facility security clearance (Secret)	Secret
Classified	Confidential	Facility security clearance (Confidential)	Secret
Protected	Protected C	Designated organization screening	Enhanced reliability status
Protected	Protected B	Designated organization screening	Enhanced reliability status
Protected	Protected A	Designated organization screening	Reliability status